COMUNE DI LOIRI PORTO SAN PAOLO
Provincia di Olbia-Tempio

REGOLAMENTO SULLE NORME DI COMPORTAMENTO PER L'ACCESSO E L'UTILIZZO DEI SISTEMI INFORMATIVI, DELLE RISORSE INFORMATICHE, DEL SERVIZIO INTERNET E DEL SERVIZIO DI POSTA ELETTRONICA.

Approvato con Deliberazione del Consiglio comunale N. 62 del 28/09/2010, su proposta N. 64 del 15.09.2010 del Responsabile del Servizio Informatico Dott. Gianluca Cocco.

PREMESSA

L'informatizzazione delle Pubbliche Amministrazioni, avviata nei primi anni novanta, ha raggiunto un livello di diffusione tale che l'espletamento delle mansioni dei pubblici dipendenti passa quasi esclusivamente per l'utilizzo di tecnologie informatiche e telematiche.

Tale diffusione ha determinato notevoli vantaggi, innalzando gradualmente i livelli di economicità, efficienza ed efficacia dell'azione amministrativa, ma ha anche generato una considerevole esposizione al rischio di un utilizzo distorto delle stesse tecnologie.

In particolare, da un lato si rende necessario garantire che il perseguimento delle finalità istituzionali mediante l'utilizzo dei dati personali altrui sia ancorato all'osservanza del c.d. principio di necessità, per il quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

D'altra parte, vi è l'esigenza dell'Ente di assicurare, mediante l'identificazione di norme comportamentali e di controllo, che l'utilizzo delle dotazioni informatiche sia improntato al mero perseguimento degli obiettivi assegnati a ciascun utilizzatore, prevenendo e perseguendo qualunque condotta contraria agli obblighi di diligenza, correttezza e riservatezza, pacificamente estendibili, nonostante la loro derivazione civilistica, al pubblico impiego.

Su queste basi nasce, pertanto, l'esigenza di dotarsi di un Regolamento sul corretto utilizzo di tutte le dotazioni informatiche che contenga, oltre ai richiami sulle principali prescrizioni previste dalla legislazione nazionale, le necessarie integrazioni normative correlate alle dinamiche peculiari dell'Ente.

Tale Regolamento è rivolto sostanzialmente a tutti gli utilizzatori delle apparecchiature informatiche in dotazione al Comune di Loiri Porto San Paolo, che hanno il dovere di conoscerlo in ogni sua parte, al fine di acquisire la necessaria cognizione sull'importanza di improntare l'utilizzo della propria postazione di lavoro alla massima correttezza e alla piena osservanza delle disposizioni dallo stesso contemplate.

Loiri Porto San Paolo, 15 settembre 2010

Il Responsabile del Servizio Informatico
Dott. Gianluca Cocco

INDICE

ART. 01 – CAMPO DI APPLICAZIONE

1. Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori del Comune ai quali è consegnata la strumentazione d'ufficio disponibile, a prescindere dal rapporto contrattuale con lo stesso intrattenuto.
2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura può anche venir indicata quale "incaricato del trattamento".

ART. 02 – DEFINIZIONI

1. **TITOLARE DEL TRATTAMENTO DEI DATI**: Ai sensi dell'art. 28 del D.Lgs. N. 196/2003, nonché del provvedimento del Garante per la protezione dei dati personali del 14/06/2007, per titolare del trattamento dei dati deve intendersi l'Ente nel suo complesso;
2. **RESPONSABILE DEL TRATTAMENTO DEI DATI**: secondo quanto indicato nell'art. 4, comma 1, lett. g), D.Lgs. N. 196/2003 per Responsabile del trattamento si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali";
3. **INCARICATI DEL TRATTAMENTO DEI DATI:** secondo quanto indicato nell'art. 4, comrna 1, lett. h), D.Lgs. 196/2003 per Incaricati del trattamento si intendono le persone fisiche autorizzate dal titolare o dal responsabile a compiere operazioni di trattamento dei dati personali;
4. **UTENTE INTERNET:** persona, all'interno dell'Ente, autorizzata ad accedere al servizio internet per la navigazione dei siti ritenuti utili al perseguimento delle finalità istituzionali;
5. **UTENTE DI POSTA ELETTRONICA:** persona, all'interno dell'Ente, autorizzata ad accedere al servizio di posta elettronica;
6. **UTENTE DI POSTA ELETTRONICA CERTIFICATA**, persona all'interno dell'ente che sia mittente o destinatario di posta elettronica certificata;
7. **WHITE LIST:** elenco di siti direttamente e immediatamente accessibili da parte di tutti gli utenti internet;
8. **BLACK LIST:** elenco di siti non accessibili da nessun utente;
9. **INTERNET PROVIDER:** azienda che fornisce al Comune il canale di accesso alla rete internet;
10. **POSTAZIONE DI LAVORO:** personal computer e relative periferiche collegate alla rete comunale, tramite i quali l'utente accede ai servizi;

11. **LOG:** archivio delle attività di consultazione in rete.

ART. 03 – UTILIZZO DEL PERSONAL COMPUTER

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio Responsabile d'Area;

2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza, evitando la sua divulgazione. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda e per lo screen saver. Non è consentita l'attivazione o la modificazione della password di accensione (bios);

3. Gli Incaricati del trattamento dei dati sono responsabili della custodia e dell'utilizzo diligente e consapevole delle proprie credenziali di autenticazione che devono essere gestite attenendosi alle seguenti istruzioni:

a) La parola chiave, assegnata a ciascun incaricato, è composta da un numero minimo di otto caratteri alfanumerici;

b) La parola chiave assegnata, deve essere prontamente e autonomamente sostituita dall'incaricato al primo utilizzo e successivamente modificata con cadenza almeno semestrale ovvero trimestrale nell'ipotesi di trattamento di dati sensibili o giudiziari;

c) All'interno di ciascuna Area/Servizio in cui si articola l'Ente, la parola chiave deve essere consegnata, in busta chiusa, al Responsabile del trattamento dei dati affinché proceda alla custodia delle credenziali;

d) La password non deve contenere riferimenti, diretti o indiretti, agevolmente riconducibili all'incaricato;

e) L'incaricato, nella scelta della propria password, deve utilizzare preferibilmente anche caratteri speciali e lettere maiuscole e minuscole;

f) La parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;

g) L'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare;

h) Qualora, in caso di prolungata assenza o impedimento dell'incaricato, così come espressamente prevede la Regola 10 contenuta nell'Allegato B al D.Lgs. 196/03, ci sia la necessità di accedere ai dati ed agli strumenti elettronici per esclusive necessità di operatività e di sicurezza del sistema, è necessario presentare una richiesta scritta e motivata al Responsabile del trattamento dei dati il quale, al rientro in servizio dell'incaricato assente ovvero impedito, provvederà ad informarlo dell'accaduto affinché si possa procedere, senza indugio, alla sostituzione della parola chiave;

i) Le credenziali di autenticazione individuali per l'accesso all'elaboratore ovvero alle applicazioni, non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Se un utente dovesse avere la necessità di trattare gli stessi dati o di usare le stesse procedure alle quali può accedere un collega, dovrà richiedere, al Responsabile del Servizio Informatico ovvero al personale all'uopo preposto, che gli siano assegnate le proprie credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti;

l) Se l'incaricato sospetta che le proprie credenziali di autenticazione abbiano perso il requisito della segretezza (ad es. perché crede che queste siano conosciute anche da altri colleghi) è tenuto immediatamente a procedere al cambio della parola chiave;

4. Il dipendente, preso atto che, la conoscenza della password da parte di terzi consente agli stessi I'accesso all'elaboratore, l'utilizzo dei relativi servizi in nome dell'utente titolare e I'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi (visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi ecc.), si impegna a:

- non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- non lasciare incustodita ed accessibile la propria postazione una volta che sia avvenuta I'autenticazione con le proprie credenziali;
- conservare e custodire la password nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti casualmente conoscenza;
- mantenere la corretta configurazione del proprio elaboratore non alterando le componenti hardware e software predisposte né installando ulteriori software non autorizzati;

5. Qualunque azione o attività esercitata mediante l'utilizzo del codice identificativo e della password assegnate, è ascritta in via esclusiva all'utente assegnatario delle credenziali di autenticazione che sarà

chiamato a rispondere delle attività eseguite. L'utente è civilmente responsabile di qualsiasi danno arrecato al Comune di Loiri Porto San Paolo, all'internet provider e/o a terzi in violazione di quanto espressamente previsto dalla norma e di quanto indicato nel presente regolamento. L'utente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua parola chiave, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico e il buon costume così come definiti dalla giurisprudenza più recente. La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dai vigenti Contratti Collettivi di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

6. Il Responsabile del Servizio Informatico e i suoi collaboratori, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà di monitorare lo spazio occupato dalle caselle di posta elettronica sul server e informare gli utilizzatori circa l'opportunità di liberare spazio, cancellando alcuni messaggi, quando lo spazio libero si approssima a zero;

7. Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del Servizio Informatico, previa richiesta scritta da parte del Responsabile dell'unità cui è assegnato il PC. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree, deve essere comunque richiesta per iscritto l'autorizzazione preventiva al Responsabile del Servizio Informatico, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Ciò al fine di scongiurare il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi;

8. Non è consentito all'utente ed ai Responsabili modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita del Responsabile del Servizio Informatico;

9. Ogni Responsabile ha l'obbligo di verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati;

10. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password;

11. Non è consentita l'installazione sul proprio PC o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili, telefoni cellulari, PDA ed apparati in genere), se non con l'autorizzazione espressa del Responsabile del Servizio Informatico, previa richiesta scritta da parte del Responsabile dell'unità cui è assegnato il PC o il segmento di rete LAN;

12. Agli utenti incaricati del trattamento dei dati sensibili è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CDRom, Nastri) una volta non sia possibile rendere irrecuperabili i dati in essi contenuti. Ai sensi del Dlgs 196/03 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'ente se non disciplinate da appositi protocolli di intesa;

13. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile del Servizio Informatico nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 5 del presente Regolamento relativamente alle procedure di protezione antivirus;

14. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

15. E' vietato rimuovere, danneggiare deliberatamente o asportare componenti hardware;

16. E' vietato accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;

17. Il personale è tenuto ad osservare le direttive del Responsabile del Servizio Informatico volte garantire il corretto funzionamento delle procedure di back-up;

18. E' vietato utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi privi di regolare licenza) o altre porzioni di codice maligno e/o altro materiale non autorizzato;

19. E' vietato copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto d'autore (documenti, files musicali, immagini, filmati e simili) di cui l'ente non abbia acquisito i diritti;

ART. 04 - UTILIZZO DI PC PORTATILI

1. Il dipendente al quale sia stato assegnato dall'Amministrazione un elaboratore portatile, è responsabile dello stesso e deve custodirlo con diligenza sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro;

2. Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in Rete;

3. I PC portatili utilizzati all'esterno (convegni, corsi, sovra luoghi etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni;

ART. 05 - PROCEDURE ANTIVIRUS

1. I dati personali trattati dall'Ente sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;

1.1 Sulla base dell'analisi dei casi, degli incidenti, delle diverse tipologie di virus e worm circolanti, delle modalità con cui si propaga un'infezione all'interno di un contesto lavorativo, gli esperti del settore hanno formulato un elenco di raccomandazioni utili per la prevenzione e la protezione dei dati che ogni dipendente del Comune di Loiri Porto San Paolo dovrà osservare:

- consultare, esaminare e diffondere messaggi specializzati di "Virus Alert";
- nella posta elettronica, quando si introducono allegati, nel caso vengano inviati documenti scritti con MS Word, è bene usare il formato RTF e non quello .Doc;
- configurare le schermate in modo che sia possibile visualizzare l'estensione dei files;
- non aprire allegati che contengano un'estensione doppia;
- in caso di ricezione di una e-mail con oggetto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato;
- non considerare le icone mostrate dagli allegati come garanzia dell'integrità del software;
- in caso di ricezione di e-mail non richieste o con contenuti insoliti, non eseguire senza aver preventivamente valutato la circostanza, collegamenti ad indirizzi web presenti nel testo della e-mail;
- controllare bene che i supporti di memorizzazione utilizzati e scambiati siano immuni da virus;
- evitare di prelevare software da sorgenti poco affidabili.

ART. 06 - PROCEDURE DI BACK-UP

1. Il Comune di Loiri Porto San Paolo è dotato di un sistema centralizzato di salvataggio dei dati immessi nella rete comunale, che il Servizio Informatico dovrà attivare quotidianamente;
2. Qualora eventuali problemi tecnici comportino una sospensione del sistema di back-up, ciascun dipendente, debitamente informato dal Responsabile del Servizio Informatico, dovrà attivare idonei meccanismi di back-up dei dati per i quali è possibile un autonomo salvataggio;
3. Le suddette misure, con cadenza almeno settimanale, dovranno inoltre essere adottate con riferimento a tutti i documenti ed alle Banche Dati eventualmente non coperti dalla indicata procedura centralizzata di back-up;

ART. 07 – UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento dell'attività lavorativa. Agli utenti è proibita la navigazione in Internet per motivi diversi da quelli funzionali all'espletamento delle proprie mansioni;
2. Tutti i dipendenti cui è assegnata dal Comune una postazione di lavoro possono utilizzare Internet, limitatamente ad una lista di siti istituzionali preventivamente individuati dal Comune (WHITE LIST) e previa identificazione dell'utente con le modalità precedentemente illustrate (credenziali di autenticazione costituite da ID UTENTE e PASSWORD);
3. La lista dei siti istituzionali fruibili (WHITE LIST) verrà progressivamente implementata e completata nel tempo ed il novero di tali siti, sarà deciso dai Responsabili d'Area dell'Ente di concerto con il Responsabile del Servizio informatico ed il Segretario Comunale;
4. L'utilizzo ampio di Internet, non limitato cioè alla lista di siti individuata come sopra (WHITE LIST), è autorizzata per ogni singolo utente da ciascun Responsabile d'Area. I responsabili delle Aree in cui si articola l'Ente sono autorizzati automaticamente a tale tipo di accesso non limitato;
5. In ogni caso, al fine di prevenire il rischio di utilizzi impropri della rete reputati non compatibili con l'attività lavorativa, il Comune utilizza un sistema di filtri che impediscono l'accesso diretto a siti che non hanno natura istituzionale (BLACK LIST);
6. Oltre a tale sistema, verrà attivata una funzione di verifica del contenuto del sito: ove tale contenuto, secondo l'impostazione di una soglia predefinita, appaia non istituzionale verrà visualizzato un messaggio che avverte l'utente; l'utente può quindi annullare la richiesta di accesso ovvero accedere al sito, previa dichiarazione di responsabilità, rendendolo da quel momento disponibile a tutti gli utenti Internet;

7. Le modalità di individuazione e di applicazione dei filtri sono decise dai Responsabili d'Area di concerto con il Responsabile del Sistema informatico ed il Segretario Comunale;

8. Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera;

9. E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili salvo i casi espressamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto;

10. E' vietata ogni forma di registrazione a siti o a mailing list i cui contenuti non siano legati allo svolgimento dell'attività lavorativa istituzionale;

11. E' vietata la partecipazione a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (ovvero nicknames) se non strettamente attinenti l'attività lavorativa svolta;

12. E' vietata tassativamente la navigazione in siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti oltraggiosi, discriminatori o che offendano il comune senso del pudore.

13. Al dipendente non e consentito:

- servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività esercitate in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- scaricare software dalla rete se non espressamente autorizzato dal Responsabile del Servizio Informatico dell'Ente;
- utilizzare internet provider diversi da quello ufficiale del Comune e connettere stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente Regolamento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

ART. 08 – UTILIZZO DELLA POSTA ELETTRONICA

1. L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Comune assegna una casella di posta personale e nominativa;

2. La casella di posta elettronica istituzionale è uno strumento di lavoro che deve pertanto essere utilizzato esclusivamente per esigenze connesse all'attività lavorativa. Non sono ammessi utilizzi diversi o privati dell'indirizzo. I dipendenti ai quali è assegnata, sono responsabili del corretto utilizzo della stessa;

3. Si evidenzia che, esclusi i casi in cui sia possibile avvalersi di una utenza di posta elettronica certificata unitamente alla apposizione della firma digitale sul documento trasmesso, i sistemi di posta elettronica non consentono di garantire circa la riservatezza delle informazioni trasmesse. Per questa ragione, si raccomanda ai dipendenti di non inoltrare, con questo mezzo, informazioni e dati classificabili come "sensibili" ovvero "giudiziari" ai sensi dell'art.4, comma 1, lettere d) ed e), D.Lgs. N. 196/2003;

4. E' fatto divieto di utilizzare le caselle di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività svolta per I'Ente, salvo diversa esplicita autorizzazione in tal senso;

5. La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente i documenti inutili e gli allegati ingombranti;

6. E' vietato utilizzare il servizio di posta elettronica istituzionale per inoltrare catene telematiche, appelli, petizioni, giochi, scherzi, barzellette, e altre e-mail che non abbiano attinenza con l'attività lavorativa. Se si dovessero ricevere messaggi di tale tipo, è necessario informare con immediatezza il proprio Responsabile e, nel caso di messaggi potenzialmente idonei a compromettere la sicurezza informatica, il Responsabile del Sistema Informatico. In ogni caso, è fatto espresso divieto attivare gli allegati di tali messaggi;

7. E' vietato utilizzare tecniche di "mail spamming", ossia di invio massiccio di comunicazioni a liste di utenti non istituzionali. E' parimenti vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi, macro, scripts);

8. Al fine di recepire le linee guida dettate dal Garante per la protezione dei dati personali in materia di posta elettronica nel rapporto di lavoro, I'Ente provvederà a mettere a disposizione di ciascun dipendente apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenza programmata dal servizio dell'utente, messaggi di risposta che avvisino il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura (coordinate elettroniche o telefoniche di un altro soggetto o altre utili modalità di contatto con la struttura). In caso di assenza non programmata e nelle more dell'attivazione della procedura di cui sopra, l'utente può delegare un altro dipendente dell'ufficio (fiduciario) a verificare il

contenuto dei messaggi e ad inoltrare al Responsabile dell'Area quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa dell'Ufficio.

ART. 09 – UTILIZZO DELLA POSTA ELETTRONICA CERTIFICATA (P.E.C.)

1. Il Comune di Loiri Porto San Paolo è dotato di un indirizzo di posta elettronica certificata che consenta all'Ente di certificare l'invio e la ricezione di documenti informatici. La relativa casella è gestita dal Servizio Protocollo;

2. Sarà cura del proprio gestore di posta fornire all'utente della P.E.C. una ricevuta attestante la prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione;

3. Ogni Area dell'Ente, mediante il proprio Responsabile, potrà chiedere, sentito il Responsabile del Servizio Informatico, l'attivazione di un indirizzo di posta elettronica certificata funzionale all'espletamento delle relative attività;

4. Ai sensi dell'art. 3 del D.P.R. 68/2005, il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore;

5. L'Ente adotta adeguate forme di pubblicità dei propri indirizzi di P.E.C. al fine di favorirne il loro utilizzo prioritario;

6. Gli uffici dell'Ente, prima di inviare un documento con le ordinarie modalità di spedizione devono sincerarsi che l'invio non possa avvenire mediante P.E.C.;

7. L'Amministrazione comunale si riserva di effettuare periodici controlli tesi a verificare gli eventuali aggravi di spesa ascrivibili al mancato utilizzo prioritario della P.E.C. da parte dei Responsabili d'Area;

8. I Bandi di concorso e di gara e tutti gli Avvisi pubblici attraverso i quali i cittadini possono inoltrare la documentazione prescritta dagli stessi devono contemplare la spedizione dei documenti mediante l'utilizzo di regolare P.E.C.. La mancata indicazione nei suddetti Bandi ed Avvisi di tale modalità di spedizione non potrà costituire una preclusione per il cittadino che intenda optare per la stessa;

9. Per quanto non contemplato dal presente Regolamento si rinvia alle disposizioni contenute nel D.P.R. 68/2005 e nel D.Lgs. 82/2005 e ss.mm.ii;

ART. 10 - MONITORAGGIO E CONTROLLI

1. Il Comune può avvalersi di sistemi di controllo sul corretto utilizzo degli strumenti di lavoro (che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori) esclusivamente nel rispetto di quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 n. 13, di quanto disposto dagli artt. 2 e 15 della Costituzione, dall'art. 616, quarto comma, C.P. e dall'art. 49 del Codice dell'amministrazione digitale;

2. In particolare l'Ente, nell'effettuare controlli sull'uso degli strumenti elettronici eviterà un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata;

3. Le comunicazioni effettuate attraverso il servizio di posta elettronica sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Comune, dell'internet provider o da parte di altri soggetti;

4. Le dichiarazioni di responsabilità effettuate dagli utenti Internet per visualizzare e rendere da quel momento disponibile il sito/dominio, secondo quanto disposto dal punto 5. del presente Regolamento, sono a disposizione del Responsabile del Sistema Informatico dell'Ente;

5. Le attività sull'uso del servizio di accesso ad Internet vengano automaticamente registrate in forma elettronica attraverso i LOG di sistema. Il trattamento dei dati contenuti nei LOG, può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività;

6. I dati anonimi aggregati, riferibili all'intera struttura o a sue Aree/Servizi, sono a disposizione dell'Ufficio Personale e del Responsabile del Sistema Informatico per le valutazioni di competenza che riguardano:

- per ciascun sito/dominio visitato le informazioni sul numero di utenti che lo visitano, sul numero delle pagine richieste e sulla quantità dei dati scaricati;
- per ciascun utente le informazioni sul numero di siti visitati, sulla quantità totale di dati scaricati e sulle postazioni di lavoro utilizzate per la navigazione.

7. I dati personali contenuti nei LOG possono essere trattati esclusivamente in via eccezionale e nelle ipotesi tassativamente di seguito indicate:

- per rispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;

- su richiesta del Responsabile del Servizio Informatico, limitatamente al caso di utilizzo anomalo degli strumenti informatici da parte degli utenti di una specifica Area/Servizio (rilevabile esclusivamente dai dati aggregati) reiterato nel tempo, nonostante un esplicito avviso circoscritto e rivolto ai dipendenti afferenti all'Area/Servizio coinvolto e un espresso invito agli stessi utenti ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;

8. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 90 giorni, e sono periodicamente cancellati automaticamente dal sistema;

9. I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

ART. 11 - INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO DI ACCESSO AD INTERNET

1. Eventuali interruzioni del servizio di accesso ad Internet sono comunicate agli utenti.

2. Ai sensi del presente Regolamento, l'utilizzo del servizio di accesso ad internet cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o di collaboratore autorizzato all'uso;
- se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti istituzionali;
- se vengono sospettate manomissioni e/o interventi sull'hardware e/o sul software dell'utente, impiegati per la connessione e compiuti eventualmente da personale non autorizzato;
- in caso di accesso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

ART. 12 – SANZIONI

1. Il presente regolamento viene consegnato a ciascun dipendente/utilizzatore del Comune di Loiri Porto San Paolo, che firma per ricevuta. Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni".

2. La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i Responsabili d'Area, o il Segretario comunale nei confronti di questi ultimi, previo espletamento di un procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, nonché attivare tutte le azioni civili e penali consentite.

ART. 13 – MODIFICHE ED INTEGRAZIONI

1. Ogni Responsabile d'Area, di concerto con l'Assessore di riferimento, può proporre al Responsabile del Servizio Informatico di sottoporre al massimo consesso civico l'approvazione di modifiche ed integrazioni al presente regolamento;

2. La mancata formalizzazione delle proposte da sottoporre al Consiglio da parte del Responsabile del Servizio Informatico non preclude che le stesse vengano autonomamente presentate dal Responsabile d'Area interessato alle modifiche e/o integrazioni;

3. Il Responsabile del Servizio Informatico effettua annualmente una ricognizione sul grado di attualità delle disposizioni contenute nel presente Regolamento, nonché della loro adeguatezza alle dinamiche interne dell'Ente, proponendo, qualora lo ritenga opportuno e necessario, una rivisitazione dello stesso al Consiglio comunale.

ART. 14 – ENTRATA IN VIGORE E PUBBLICITA'

1. Il regolamento entra in vigore con l'avvenuta esecutività della Deliberazione di approvazione da parte del Consiglio comunale;

2. Con l'entrata in vigore del presente regolamento tutte le eventuali disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti;

3. Copia del regolamento è pubblicata sul sito ufficiale del Comune di Loiri Porto San Paolo, nelle sezioni "Albo Pretorio" e "Regolamenti";